

# Cybersecurity Incident Report:

## Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that: There is an error in the packet request

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:

The port noted in the error message is used for: DNS Servers

The most likely issue is: port

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: 1:24pm

Explain how the IT team became aware of the incident: After I ran ICMP protocol

Explain the actions taken by the IT department to investigate the incident:

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

Note a likely cause of the incident: